frontiers | Frontiers in Education

TYPE Original Research
PUBLISHED 07 October 2025
DOI 10.3389/feduc.2025.1689273

Cybersecurity in accounting education: accounting academics' perspectives

Pranisha Rama*†, Ben Marx† and Rozanne Smith†

Department of Accounting, University of Johannesburg, Johannesburg, South Africa

Check for updates

OPEN ACCESS

EDITED BY
Ramon Ventura Roque Hernández,
Universidad Autónoma de Tamaulipas, Mexico

REVIEWED BY
Noble Lo,
Lancaster University, United Kingdom
Firas Mustafa,
Alnoor University, Iraq

*CORRESPONDENCE
Pranisha Rama
✉ pranishar@uj.ac.za

†These authors have contributed equally to this work

RECEIVED 20 August 2025
ACCEPTED 15 September 2025
PUBLISHED 07 October 2025

CITATION
Rama P, Marx B and Smith R (2025) Cybersecurity in accounting education: accounting academics' perspectives. *Front. Educ.* 10:1689273.
doi: 10.3389/feduc.2025.1689273

Introduction: Cyberattacks continue to intensify and are currently the top global technological risk. This global increase in cyberattacks and the growing dependence on digital platforms have also heightened the significance of cybersecurity within the accounting profession. As future custodians of sensitive financial data, accounting students must possess both the technical understanding and the practical skills to prevent such threats. Given the importance of the digital economy within the accounting profession, accounting curricula often do not include cybersecurity education, resulting in accounting students being inadequately prepared. This research aimed to fill this gap by formulating cybersecurity education guidelines through competencies for an accounting curriculum and is designed to be incorporated into various modules throughout the curriculum.

Methods: Content analysis was conducted as part of the literature review to determine which competency frameworks of accounting professional bodies were relevant and which cybersecurity competency statements were to be included in the questionnaires as part of the quantitative study. While the study is predominantly quantitative in nature, the incorporation of participant comments adds a minor qualitative dimension, making the overall design descriptive with supportive qualitative elements. The questionnaire was distributed to accounting academics, and 41 responses were received.

Results: The findings from this study indicate that accounting academics lack knowledge around cybersecurity and do not know how to incorporate the topic into the curriculum. Academics have also viewed cybersecurity as an important component of the accounting curriculum, given its emphasis within the digital economy.

Discussion: This study contributes to the development of the accounting curriculum and highlights the importance in developing cybersecurity skills in future accounting professionals which can be incorporated by making use of real-life case studies, using experts from the cybersecurity industry.

KEYWORDS

cybersecurity, cybersecurity education, accounting education, cybersecurity competencies, accounting students, accounting curriculum, accounting academics

Introduction

Cyberattacks have become widespread and will continue to escalate as technology rapidly advances, creating an ever-evolving landscape of threats that challenge the security measures of organizations and individuals alike (Chizanga et al., 2022). The cyberattack landscape has intensified over the years, with the attack on Estonia (a country in Northeastern Europe) in 2007 being one of the first mass-scale cyberattacks. This attack lasted 22 days and temporarily impacted the degradation or loss of service to many commercial and government servers (Kumar et al., 2016). The upsurge in cyberattacks has created several challenges, but it has also presented several opportunities. One such area of opportunity is cybersecurity, which offers several employment opportunities and roles required in combating cyberattacks (Mijwil et al., 2023). The prediction is that millions of cybersecurity specialists will be needed in the foreseeable future with accounting firms globally including cybersecurity as a service offering to respond to the demand for cyber specialists (Mendlowitz, 2022). There is a huge demand for cybersecurity skills, and this trend is expected to grow in the foreseeable future and has been listed as one of the top 10 competency areas of the future (ACCA Global, 2022; KPMG, 2022). Cybersecurity education and knowledge need to be developed to combat the escalating issue of cyberattacks, and this attests to cybersecurity education being a priority in dealing with ongoing cybersecurity concerns.

Accounting professionals should be educated on cybersecurity, allowing it to become an integrated area of expertise so they can contribute more effectively to the development and implementation of robust security protocols, ultimately helping to safeguard their organizations against the ever-growing threats posed by cyberattacks (Tauchman, 2021). In a study that investigated whether aspiring and professional accountants understand the benefits and security challenges brought by emerging technologies, Rîndaşu (2017) found that accounting professionals face multiple knowledge gaps when it comes to cybersecurity and computer systems. To fill this critical knowledge gap, it is essential to provide accounting students with comprehensive education in cybersecurity, enabling them to thoroughly understand this increasingly important concept (Meyer, 2021). This can be achieved by including cybersecurity in the accounting curriculum at the university level. By doing so, students will have the opportunity to engage with essential cybersecurity topics throughout their studies, allowing them to build a strong understanding of how these principles intersect with accounting practices.

Accounting students must have the required skills, knowledge, and education to meet employer expectations and the competencies required by accounting professional bodies. Moreover, for accounting students to stay relevant and fit for purpose, cybersecurity is one area that can increase the relevance of accounting students (Albuquerque and Dos Santos, 2023; Bartley, 2023). Meyer (2021, np) states that:

> *"Another hurdle is the fact that there's no real consensus on how universities should teach cybersecurity… But all too often, cybersecurity is not included in accounting programs at all."*

While research on cybersecurity education has been conducted, there remains a gap in the literature specifically addressing cybersecurity education for accounting students from an academic perspective (Roohani and Zheng, 2019; Boss et al., 2022). This raises concerns regarding the extent to which cybersecurity has been integrated into the accounting curriculum by accounting academics.

The increasing prevalence of cybersecurity threats continues to escalate within the accounting profession, and given that accounting professionals are considered as custodians of financial data, it is important to equip accounting students with the required cybersecurity knowledge. While the importance of cybersecurity is recognized in the profession, little is known about how accounting academics incorporate this into the curriculum. Thus, this study aims to investigate accounting academics' perspectives on the inclusion of cybersecurity education within the accounting curriculum, assess the extent to which it has been integrated, and explore their preferred teaching methods for effectively delivering cybersecurity content. This study follows a single case study design to explore cybersecurity competencies within the accounting curriculum within a higher education. This research is guided by the following questions:

1. What cybersecurity competencies should be incorporated into the accounting curriculum?
2. How do accounting academics incorporate cybersecurity into the accounting curriculum?
3. What challenges and opportunities do accounting academics identify in integrating cybersecurity into accounting curricula?

Literature review

Theoretical framework

Curriculum theory focuses on developing curricula that reproduce learning opportunities and broaden them through effective design (Kelly, 2009). This theory is applied to all educational institutions, including higher education, and thus would apply to this study (Gurin et al., 2002). Curriculum development refers to how curriculum theory contributes to the development of curriculum texts and syllabuses and produces research of relevance to such developmental processes, which entails the scrutiny and evaluation of the educational curriculum to comprehend its arrangement, substance, conveyance, and results (Syomwene, 2020). It encompasses various approaches and philosophies about how curricula should be designed, implemented, and evaluated, encapsulating education's core focus.

Saadeh (2019, p. 9) refers to curricula as the "heart" of education. The curriculum is the necessary guide for thinking, laying the groundwork for purpose and practice. Curriculum theory plays a crucial role in the incorporation of cybersecurity education into the accounting curriculum, which focuses on building and evaluating a curriculum that effectively combines cybersecurity principles pertinent to the accounting sector. Curriculum theory provides a framework for designing, implementing, and evaluating educational programs (Khan and Law, 2015) and emphasizes the principles and practices of curriculum development, providing an education structure that can be used in the context of cybersecurity education. Academics' perspectives are a pertinent factor in the development of the curriculum.

Cybersecurity education

When a curriculum considers cybersecurity as part of its offering, educating accounting students on cybersecurity threats and risks ensures that accounting students are equipped with the relevant knowledge required to manage cybersecurity challenges that organizations face and also meet employer expectations (Fakoya-Michael and Fakoya, 2020). Zhang et al. (2020) argue that not addressing areas such as cybersecurity in the accounting curriculum reduces the employability and work-readiness of accounting graduates. Gulin et al. (2019) conducted a study that focused on the challenges that digitalization brings to the accounting profession, and found that digitalization will require universities to change and modify their education programs to prepare accounting students for work in the modern environment, along with automation and digitization. Furthermore, as digitalization continues to transform the accounting profession, universities must update their programs to prepare students for the evolving demands of a modern, automated, and digitized work environment (Berniak-Wozny et al., 2023).

An effective curriculum design will equip students with the necessary technical skills, knowledge, and competency to meet the demands of the industry (Hadgraft and Kolmos, 2020). A study that focused on the COVID-19 pandemic, which required curricula to adjust to a new way of delivering content, Ali (2020) indicated that a curriculum must be able to adjust to a constantly evolving technology environment to remain pertinent. In its reports on future skills for accounting students, The AICPA (2021) asserts that universities have a critical responsibility to equip students with relevant and up-to-date technology, including specialized courses in cybersecurity, to align with the evolving expectations of employers and to ensure that graduates are well-prepared for the demands of the modern workplace.

The accounting curriculum is already fully packed; however, cybersecurity is a topic that can easily be incorporated across all aspects of the accounting curriculum (Pasewark, 2021). Researchers argue that cybersecurity should not be seen as another topic or add-on, but as part of an accounting curriculum where cybersecurity should not be an entirely new course; it should be introduced, emphasized, and followed up on throughout the curriculum (Corriss, 2010; Montgomery, 2022; Paulsson and Brady, 2022). A typical accounting curriculum comprises four core technical modules, namely accounting, financial management, taxation, and auditing, also considered majors in specialist areas (Barac and Du Plessis, 2014). The first step is to understand if the current curriculum includes technically relevant subject matter, and once a curriculum is understood, it is important to identify areas where there is an opportunity to include the relevant subject matter (Crean and Carroll, 2022; Leidig and Salmela, 2022). Gaining an in-depth understanding of the curriculum is integral to successfully integrating the new subject matter. Meyer (2021) and Mujiono (2021) both suggest that cybersecurity education should be embedded throughout the curriculum within core modules, due to the unique nature of each module and the outcomes linked to each module (Mujiono, 2021). These modules are technical, and the relevant digital skills associated with each specific module can be strategically introduced and embedded throughout the curriculum to ensure that students develop a deep and practical understanding of the digital competencies required (Kee, 2024). Often the curriculum includes other supporting modules that include business information systems, ethics, commercial law, business management and statistics (Mphahlele, 2023).

Boss et al. (2022) investigated the integration of cybersecurity education for accounting students in the USA, particularly emphasizing the specific criteria mandated in the country. The proposed inclusion does not address the importance of cybersecurity awareness of threats regarding attacks targeting students and focuses on cybersecurity technical competency aspects. The study concludes that accounting curricula worldwide should integrate cybersecurity as a fundamental component of accounting education, reflecting the growing importance of increasingly sophisticated cyber threats.

Universities are responsible for preparing students for the workplace, and accordingly, the inclusion of cybersecurity education is important in ensuring that accounting graduates are adequately prepared for the cyber challenges organizations face (Baker, 2016; Cameron and Marcum, 2019). Graduate unemployment has been a serious concern, and one of the contributing factors is that graduates are not able to meet industry needs in terms of skills required, thus requiring universities to understand what is needed for an individual to be skilled enough once they enter the workplace (Alam, 2021; Mgaiwa, 2021). A study by Ebaid (2022) focusing on exploring accounting students' attitudes toward integrating forensic accounting into accounting education, indicates that students strongly desire to study cybersecurity as part of an accounting curriculum. Adding cybersecurity to an accounting curriculum also increases employability, ensuring that graduates succeed long-term (Ghani and Muhammad, 2019).

Employers seek to hire graduates with expertise in cybersecurity, and given the growing need for cybersecurity professionals, the accounting curriculum can play a role in developing this skillset (Matthysen and Harris, 2018; Burrell, 2022; Kisaalita et al., 2022). Universities play a pivotal role in preparing students to be employable and providing relevant education and knowledge. Accounting students must be prepared for a digital environment, and accounting curricula are required to adequately prepare students for this transition, with employers preferring work-ready candidates (Jackson and Meek, 2021). Technical knowledge on cybersecurity should be taught throughout the curriculum, for example, providing theoretical knowledge through lectures and practical aspects through an assignment (Jeffryes and Lafferty, 2012).

Cybersecurity is an area of expertise being sought after by many organizations; however, the accounting curriculum has yet to respond to this (Aldawood and Skinner, 2019). There is currently a shortage of cybersecurity programs and even fewer programs directed toward accounting students, given the importance and emphasis of cybersecurity (Douglas and Gammie, 2019; Sutherland, 2020; van Oorschot, 2020; Rajgopal, 2021). Grech (2022) found a strong need to include cybersecurity as part of an accounting curriculum due to the impact cybersecurity has on business decisions, of which accounting students must be a part. Accounting students would benefit from cybersecurity as part of the curriculum, as this allows them to understand data better, thereby assessing risks adequately (Srinivasan, 2013).

Rebele and St. Pierre (2019) observed that accounting academics are generally resistant to change and are not skilled in an area like cybersecurity, which could further contribute to the non-inclusion of cybersecurity within an accounting curriculum. Technological resistance is another factor that hinders curriculum development, and educators are required to stay up to date with these changes (Kee, 2024).

The accounting curriculum must be reassessed, reducing content in more traditional areas, e.g., Financial Management, and adding more content on Accounting Information Systems (AIS), including cybersecurity, which can aid in an already loaded curriculum (Churyk et al., 2024). Accounting Information Systems is a module that can offer deep coverage of digital skills (Kee, 2024). The IESBA (International Ethics Standards Board for Accountants) has increased focus on data and the governance of how this data is managed, thus emphasizing the importance of cybersecurity ethics, and has been included as such in accounting competency frameworks for accounting students (IESBA, 2022). This is to ensure that accountants are not faced with legal and ethical challenges; therefore, the IESBA has added ethics in technology, specifically in cybersecurity (Loots et al., 2024). This has called for increased awareness of cybersecurity for accounting professionals and should be included in the curriculum as such. Technical content in core modules, as suggested by Boss et al. (2022), is included in Table 1.

TABLE 1 Technical cybersecurity content.

Subject matter area	Explanation	Subject area
Cybersecurity disclosures in financial reporting	Specific accounting disclosures are required regarding cybersecurity, and stakeholders expect that these are disclosed appropriately for transparency.	• Accounting
Cybersecurity breach in financial audit	Due to the financial impact of cybersecurity, audit teams are expected to have education about the impact on the audit and how this may affect the audit, and design procedures accordingly.	• Auditing
Tax preparers protecting personally identifiable information	Tax preparers must protect client information due to the risk of a breach.	• Taxation
Calculate cybersecurity breach costs	Accounting professionals are required to have knowledge of accuracy in calculating the cost of a breach.	• Financial Management/ Cost Accounting
Classifying and measuring cybersecurity breach costs	The classification of costs is important in reporting. - Direct costs incurred when dealing with the breach after detection, including engaging forensic experts, hiring law firms, and offering identity protection services to breach victims. - Indirect costs are those expenses connected with internal resources, including employees' time, effort, and other resources necessary to cover the losses from the data breach.	• Financial Management/ Cost Accounting

Accounting academics

Preparing accounting students adequately for market demands is crucial, and universities play a critical role in developing education to adapt to such market demands; this includes areas such as cybersecurity (Jackson et al., 2023). Universities must adapt their curricula to an ever-changing technological landscape, which will prepare accounting students better for what the employment market requires and improve their knowledge of technology, such as cybersecurity.

When a curriculum considers cybersecurity as part of its offering, educating accounting students on cybersecurity threats and risks ensures that they are equipped with the relevant knowledge to manage cybersecurity challenges that organizations face and also meet employer expectations (Fakoya-Michael and Fakoya, 2020). Not addressing areas such as cybersecurity in the accounting curriculum reduces the employability and work-readiness of accounting graduates, as it hinders their ability to meet the growing expectations of employers (Zhang-Kennedy and Chiasson, 2022). Gulin et al. (2019) found that digitalization will require universities to change and modify their education programs to prepare accounting students for work in the modern environment along with automation and digitization. Furthermore, as digitalization continues to transform the accounting profession, universities must update their programs to prepare students for the evolving demands of a modern, automated, and digitized work environment (Berniak-Wozny et al., 2023).

According to Meyer (2021) it is essential to integrate cybersecurity concepts into the accounting curriculum to ensure that accounting students are well-versed in these concepts. In a study focusing on accounting education's usefulness and long-term nature in the digital age, Tharapos (2022) found that engaging with experts in the field of cybersecurity will help accounting students by showing them how it works in real life, which is seen as a way that this area can be added to the curriculum.

Methods of teaching cybersecurity

In the twenty-first century, teaching an accounting curriculum at the undergraduate level aims to train students with a solid theoretical basis, strong practical ability and high comprehensive quality (Panja, 2018). In an accounting degree, an educator must teach the subject matter and provide education on matters that are integral to the economy. An accounting educator's responsibility is to provide not only accounting knowledge but also to teach how to stand in the globalized age of business; thus, the method of delivery is an important factor in educating accounting students. A key consideration of cybersecurity education is the method of delivery, which must be included within the accounting curriculum (Chowdhury and Gkioulos, 2023).

According to Strauss-Keevy (2014), the most effective delivery methods for accounting education are lectures, discussion, small groups and collaborative learning, case studies and examples, role-playing, and guest speakers. The conventional lecture method is a long-standing approach to instruction that emphasizes the transfer of knowledge rather than the process of learning. The lecture method may be suitable for introducing and describing basic concepts around cybersecurity.

Students and professional accountants are more likely to develop judgement and behavior through exposure to and discussion of cybersecurity issues with others, especially those holding alternative viewpoints (Wolk and Nikolai, 1997; Ismail and Rasheed, 2019). This helps individuals become familiar with important concepts, gain practice in using the language of cybersecurity, and develop judgement (Bressler and Pence, 2019).

Small-group learning, which develops skills in leadership, decision-making, trust-building, communication, and conflict management, is an effective method for exposing students to examples of cybersecurity issues (Jerman BlaŽič and Jerman BlaŽič, 2022). Interaction with other students and/or professional accountants in peer-led cybersecurity discussions promotes more significant learning than can be achieved individually.

The case study method effectively develops analytical skills (Ballantine and Larres, 2004; Terblanche et al., 2023). Advantages of case studies include the development of critical thinking and reflective learning skills and the integration of technical skills and knowledge that involve students and/or professional accountants in real-life events and provide insight into what it feels like to experience such problems (Bérubé and Gendron, 2022).

Methods

While the study is predominantly quantitative in nature, the incorporation of participant comments adds a minor qualitative dimension, making the overall design descriptive with supportive qualitative elements.

Prior to the questionnaire going out to academics, this questionnaire was pilot tested amongst five accounting academics, where feedback was received, and the questionnaire was adjusted accordingly. Once the questionnaire was final, this was sent out to all accounting academics within the Department of Accounting, where academics are involved in degree programs. The questionnaire was sent out via email, by the Head of the Department of Accounting to all academics. Responses were received via a Google form. The Google form required informed consent from all participants, where an academic wished not to provide content, the questionnaire did not proceed further. This questionnaire was made available for a period of 6 weeks (1 April 2024–15 May 2024). Ethical clearance was obtained to conduct this study.

The sample of academics only focused on academics that lecture on degree programs, where a total of 100 academics are working (at the time of the study). This would result is a 41% response rate. This response rate is considered as sufficient, as evidenced through various literature sources (Nulty, 2008; Cook et al., 2009; Malan and van Dyk, 2021). The inclusion criteria included academics that lecture on degreed programs, that includes bachelors programs, post graduate programs, and honors programs. Certificate, diplomas, masters and Ph.D. programs were specifically excluded for this study. Responses were received from academics teaching across all years of study, suggesting the sample is broadly representative and reducing concern about non-response bias.

This study was completed in two steps. Step one constituted a content analysis, and step two was a questionnaire based on the content analysis results that was distributed to 41 accounting academics who lecture across the accounting curriculum (from first year to postgraduate years). The academics also lectured across all modules ensuring a diverse set of responses were received.

Cybersecurity competencies were derived using literature and competency frameworks of accounting professional bodies. The researchers utilized a three-phase approach to discover and define key competencies for cybersecurity education. This systematic methodology increased reliability in coding and thematic analysis. All pertinent documents, publications, and research papers obtained from an extensive literature survey were printed and examined during the preliminary phase. The subsequent phase entailed loading the coded data into ATLAS.ti, a qualitative analysis software program that facilitates advanced data management and coding (Woods et al., 2016).

The researchers performed a second-cycle coding method, which involved consolidating, reorganizing, and improving the initial codes established in Phase 1. ATLAS.ti enabled the cross-referencing of codes and aided the identification of patterns, linkages and distinctions across various cybersecurity concepts. This stage was essential for validating preliminary findings and minimizing potential researcher bias by thorough data categorization. In the concluding step, the researcher performed a comprehensive thematic analysis. The codes generated by ATLAS.ti were analyzed and categorized into themes.

Each code was analyzed for its significance, frequency, and interrelation with other codes, forming separate themes that captured fundamental cybersecurity competencies. This approach produced 34 original codes, which were consolidated into 19 themes. The 19 themes provide the definitive compilation of recognized competencies considered for cybersecurity education for accounting students. During each phase, the researcher implemented measures to improve reliability and validity, including maintaining a comprehensive audit trail of coding decisions and holding feedback sessions with co-researchers. The researchers helped ongoing meetings where the codes were discussed and where there was a disagreement, these were discussed in detail, till consensus was achieved. The themes were then used to develop the questions that were used for the questionnaire. The questionnaire has been included in Appendix 1.

The questionnaire results were analyzed using SPSS, where quantitative data was obtained. Cronbach's alpha was used to measure reliability. This measurement indicates consistency in how participants would have answered a questionnaire. Cronbach's alpha ranges from 0 to 1, with higher values denoting higher internal consistency, where a reliable measure of anything above 0.7 is considered acceptable (Zhang-Kennedy and Chiasson, 2022). A standard deviation measure is a measure of how dispersed the data is from the mean, and an acceptable number is no more than two. It is commonly assumed by statisticians that 68% of all data points

TABLE 2 Cybersecurity competencies.

Final competency (19)	Preliminary Competency Source(s) (34)	Coding rationale for the accounting curriculum

C1. The concept of data security	Cyber threat types (1);
	Vulnerabilities and exploits (2);
	Basic data security principles (3)
		Clustered general cyber threat awareness and foundational data security concepts are covered across competency frameworks.

C2. Consequences of cyber threats and impact on investors' confidence	Consequences of breaches: Impact on stakeholders (4)	Consolidated threat consequences, emphasizing investor confidence (accounting relevance) as covered across competency frameworks.
C3. Purpose of cybersecurity governance frameworks	Risk governance principles (5)	General governance concepts merged into one overarching competency as covered across competency frameworks.
C4. NIST framework	NIST core functions (Identify, Protect, Detect, Respond, Recover) (6)	Retained as a standalone competency due to global relevance and curriculum value, covered across competency frameworks.
C5. COBIT framework	COBIT control objectives (7)	Retained as a standalone competency for accounting/audit linkages covered across competency frameworks.
C6. ISO framework	ISO/IEC 27001, ISO/IEC 27032 cybersecurity standards (8)	Retained separately for the importance in understanding covered across competency frameworks.
C7. Cybersecurity risks	Risk assessment basics: Nature of risk (9)	Created a broad competency in introducing cybersecurity risk, given the emphasis in accounting competency frameworks.
C8. Identification of cybersecurity risks	Threat identification (10); Risk recognition (11)	Focused competency on recognizing specific risks relevant to accounting.
C9. Analysis of nature and impact of risks	Risk analysis methods (12); Impact assessment (13)	Consolidated into a single analytical competency.
C10. Consequences of cybersecurity risks	Organizational consequences (14); Financial implications (15)	Refined to emphasize outcomes relevant to accounting reporting.
C11. Internal control weaknesses (cybersecurity)	Weaknesses in ITGCs (16); Weaknesses in application controls (17)	Retained as a competency highlighting vulnerabilities.

C12. Internal controls implemented over cybersecurity	Preventive (18);
	detective (19);
	corrective controls (20)
		Merged into a competency on practical internal control responses.

C13. General controls in cybersecurity	ITGCs (access, change management, operations) (21)	Grouped into a standalone competency (general IT controls).

C14. Application controls in cybersecurity	Input (22);
	processing (23);
	and output controls (24)
		Kept distinct to reflect audit/accounting teaching.

C15. Cybersecurity disclosures in financial reporting	Disclosure requirements (25); Reporting obligations (26)	Refined to the financial reporting for accounting.
C16. Cybersecurity breach in a financial audit	Audit implications of breaches (27); Auditor responsibilities (28)	Consolidated into one audit-specific competency.
C17. Protecting clients' data in tax preparation	Data privacy in taxation (29); Client confidentiality (30)	Tailored to taxation teaching contexts within cybersecurity.
C18. Classification and measurement of breach costs	Costing models (31); Financial impact measurement (32)	Collapsed into a competency linking cybersecurity with measurement.
C19. Cybersecurity violations impacting reporting requirements	Regulatory compliance (33); Reporting violations (34)	Consolidated to address reporting/accounting regulatory risks.

Source: Own compilation.

will be within +/−1SD from the mean and 95% of all data points will be within +/−2SD from the mean (Sheats and Shane Pankratz, 2002). The primary data analysis relied on quantitative descriptive statistics (such as means and standard deviations) to summarize participants' responses. In addition, a few open-ended comments provided by participants were included to enrich the findings with limited qualitative insights.

The findings are tabulated as statements that were presented to the academics in the questionnaire. The findings table uses the mean and standard deviation as a display method. The standard deviation obtained for all findings was within an acceptable range and, thus, was accepted in all cases. The questionnaire was then formulated based on the 19 competencies, where academics were presented with each competency area, and using a five-point Likert scale, were required to rank their integration of the competencies into the accounting curriculum [(1) To no extent, (2) Small extent, (3) Moderate extent, (4) Large extent, (5) Very large extent].

Table 2 provides a list of the 19 identified competencies (CIMA, 2018; Roohani and Zheng, 2019; AICPA, 2021; ACCA Global, 2022; Boss et al., 2022; SAICA, 2022; IFAC, 2023; SAIGA, 2023). Results are presented using the mean and standard deviation.

This study uses a singular case study, as this research aims to explore cybersecurity education for accounting students that can be incorporated into the curriculum through guidelines. Case study design methodology can be described as an "intensive study about a person, a group of people or a unit, which is aimed at generalizing over several units" (Heale and Twycross, 2018, p. 7). Case studies focus on complex phenomena in the natural setting to increase understanding of them by capturing the case's complexity (Johansson, 2007). This is achieved by using multiple methods to gather information. The case study method is preferred when there is little prior knowledge about the variables of interest. Case study research is an established research design that has been employed in educational innovation and project evaluation, as it is able to capture individual differences, diverse experiences or unique variations among participants (Keevy, 2022).

While case studies can be replicated, they come with some pitfalls, including results that need to be generalizable, researcher bias and even over emphasis in the detail (Greene and David, 1984). While multiple case studies are considered robust and worthy of undertaking, this study aims to provide cybersecurity education guidelines through competencies that can be incorporated into an accounting curriculum (Stake, 2013). These guidelines can then be replicated for other accounting programs.

The selected case study for this study is:

- The largest residential university, specifically for accounting students (Keevy, 2022).
- The university produces the largest number of African CAs, so it was important to consider a diverse student body, emphasizing its contribution to transformation (Rensburg, 2020; Keevy, 2022).
- The university is at the forefront of integrating 4IR into its accounting degree programs (Business Day, 2020).

Thus, the selected case study university is considered to be appropriate for this study.

Results

Table 3 provides a summary of responses from academics throughout the curriculum, and the distribution thereof.

Table 4 presents the results of the cybersecurity competencies that were presented to accounting academics.

Discussion

Academics from 1st to post graduate studies partook in the study, thereby providing responses from across the qualification as indicated in Table 3. A Cronbach's alpha of 0.981 and the highest standard deviation of 1.453 was achieved for the cybersecurity competencies section, thus acceptable in all cases.

TABLE 3 Year of study.

Year of involvement	Responses
1st year	**3**
2nd year	**15**
3rd year	**11**
BCom Accounting (Hons)—Financial Management, Internal Audit, Taxation, PGDA	**12**
Total	**41**

Source: SPSS output of questionnaire, own layout.

The findings in Table 4 reveal limited integration of cybersecurity into the accounting curriculum. The consensus among academics, with means of 1.44–2.51 indicate that cybersecurity content has been partially incorporated, though the majority of academics either disagreed or strongly disagreed with the extent of inclusion within their respective modules. These findings are expected, given that not every module is expected to deliver cybersecurity content; however, the comments obtained from academics provide further context on this finding, indicating that academics are not exactly sure how to include these competencies in their modules, which would contribute to an even lower inclusion rate.

Areas such as cybersecurity risks (mean = 2.51), data security (mean = 2.37), and the consequences of cybersecurity risks as well as general controls over cybersecurity risks (mean = 2.20) received slightly higher inclusion, suggesting these topics are recognized more within an accounting curriculum. The results indicate that most academics included these areas as part of the curriculum to some extent, ranging from a moderate to a very large extent. This finding is promising for building on the basics of cybersecurity, as part of an accounting curriculum. Qualitative comments that supporting the importance of these areas include:

> *"Cybersecurity should be prioritized in the accounting curriculum as it is a risk that forms part of the day-to-day activities of an accounting professional."*
>
> *"This is essential as accounting graduates will be working with classified information of their clients. It is important to know how to protect this information from any cyber risks."*
>
> *"In my module we only cover basic principles of the computerized environment and we only touch a bit on types of computer viruses. However we cover application and general computer controls in a large extent. Thus students should have knowledge of these controls."*

Lower scores for areas like application controls in the context of cybersecurity (mean = 2.12), internal controls over cybersecurity (mean = 2.10), and cybersecurity internal control weaknesses (mean = 2.02) were observed; however, this would be expected given that this subject matter is very module dependent, for example, it would be covered in an auditing-based module. The limited focus on the identification of cybersecurity risks (mean = 2.00) further underscores the need to strengthen foundational understanding. Just less than half of the academics who participated in the questionnaire have included

TABLE 4 Cybersecurity competencies.

Competency statements	To no extent (1)	Small extent (2)	Moderate extent (3)	Large extent (4)	Very large extent (5)	TOTAL	Mean	Standard deviation
C1 The concept of data security	14	10	8	6	3	41	2.37	1.299
C2 The consequences of cyber threats and the impact on investors' confidence	22	5	4	7	3	41	2.12	1.418
C3 The purpose of Cybersecurity governance frameworks	24	5	7	3	2	41	1.88	1.229
C4 NIST (National Institute of Standards and Technology)	31	4	3	1	2	41	1.51	1.075
C5 COBIT (Control Objectives for Information and Related Technology)	31	4	2	2	2	41	1.54	1.120
C6 ISO (International Organization for Standardization)	30	3	3	3	2	41	1.63	1.199
C7 Cybersecurity risks	12	11	7	7	4	41	2.51	1.344
C8 Identification of the type of cybersecurity risks	21	6	9	3	2	41	2.00	1.225
C9 Analysis nature and impact of cybersecurity risks	24	6	5	4	2	41	1.88	1.249
C10 The consequences of cybersecurity risks	17	8	9	5	2	41	2.20	1.249
C11 Cybersecurity internal control weaknesses	23	4	6	6	2	41	2.02	1.332
C12 Internal controls that can be implemented over cybersecurity	23	4	5	5	4	41	2.10	1.446
C13 General controls in the context of cybersecurity	21	5	5	6	4	41	2.20	1.453
C14 Application controls in the context of cybersecurity	23	3	6	5	4	41	2.12	1.452
C15 Cybersecurity Disclosures in Financial Reporting	26	8	5	1	1	41	1.61	0.972
C16 Cybersecurity Breach in a Financial Audit	28	7	4	1	1	41	1.54	0.951
C17 The importance of protecting clients' data in the process of preparing taxation calculation	24	7	6	1	3	41	1.83	1.223
C18 Classification and Measurement of Cybersecurity Breach Costs	31	5	3	1	1	41	1.44	0.923
C19 Cybersecurity violations that may impact accounting reporting requirements	30	6	3	1	1	41	1.46	0.925

these concepts in the curriculum. Comments that support this finding includes:

> *"I am also not a cyber security expert so have limited exposure and only theoretical knowledge limited to the theory around computers and application controls that I teach."*
>
> *"Cyber security is becoming increasingly important, we make the students aware of this in the module, but more can certainly be done. We lecture this as part of the module on the theory of computer environment and application controls in the auditing curriculum."*

Findings with scores below 2 indicate a low level of inclusion of advanced cybersecurity competencies within the accounting curriculum, for instance, competencies such as the purpose of cybersecurity governance frameworks (mean = 1.88) and analysis of the nature and impact of cybersecurity risks (mean = 1.88) show limited integration, suggesting that these fundamental concepts are not adequately emphasized in teaching.

Similarly, topics such as the importance of protecting clients' data in the context of tax preparation (mean = 1.83), ISO standards (mean = 1.63), and cybersecurity disclosures in financial reporting (mean = 1.61) also display minimal incorporation, reflecting a potential lack of familiarity or perceived relevance among academics. Even more concerning are the extremely low scores for highly specialized areas, such as COBIT (mean = 1.54), cybersecurity breaches in financial audits (mean = 1.54, 31%), NIST standards (mean = 1.51), cybersecurity violations affecting accounting reporting requirements (mean = 1.46), and classification and measurement of cybersecurity breach costs (mean = 1.44), which underscore significant gaps in technical and applied knowledge. Whilst academics have included these competencies, this has been included to a limited extent within the curriculum.

Comments supporting this finding include:

> *"Little is done on the governance and the various frameworks like COBIT and ISO are not dealt with at this level."*
>
> *"I have a limited understanding on how the cybersecurity affects accounting fraternities."*
>
> *"This is not covered in Accounting but I believe it forms part of other modules within the same course."*
>
> *"Accounting in general does not exclusively look into cybersecurity and I believe it would be beneficial if we start incorporating it in Accounting."*

The findings suggest that whilst cybersecurity is considered important, there is limited inclusion in the curriculum, which stems from academics not having the knowledge around cybersecurity, curriculum constraints, and academics not being used to this as a focus area. The low rate of inclusion emphasizes the importance of providing academics with guidance on the incorporation of cybersecurity.

Additional comments from academics

Whilst there is some level of incorporation in certain modules, many academics have indicated that they are not aware of how to incorporate this into their respective modules but believe that the list of competencies presented provides some level of guidance and ideas in terms of how cybersecurity can be included in the curriculum, as noted in the comments below.

> *"In the module, since the aim is to create awareness, they have not been covered, but should be and I will include elements of the above. The list touches on relevant aspects in the cybersecurity space."*
>
> *"Professionals in tax, accounting, auditing, and financial management must have a good understanding of cybersecurity competencies to effectively safeguard financial data, comply with regulations and mitigate cyber risks in today's digital environment. Continuous education and training play a significant role in keeping up to date with the evolving cyber threats and best practices in cybersecurity management. Cybersecurity should be emphasized in accounting education to produce professionals with better cybersecurity skills."*

Source: Questionnaire data.

The accounting curriculum must incorporate these competencies adequately into the curriculum, as professional bodies plan to include these competencies as part of their exams (AICPA, 2021). While the literature indicates that accounting academics are resistant to change, these guiding competencies can provide a basis for inclusion in the accounting curriculum (Rebele and St. Pierre, 2019). Students must be educated on these technical competencies, as indicated by the literature (Roohani and Zheng, 2019; Boss et al., 2022). These competencies can be spread throughout the curriculum within various modules, allowing students to gain an in-depth understanding from a basic level to a more comprehensive level (Dore and Murphy, 2022). The literature review suggests that the students need a more comprehensive understanding of governance frameworks (Roohani and Zheng, 2019).

By embedding cybersecurity competencies into the accounting curriculum, universities can equip students with the tools necessary to navigate an increasingly complex digital landscape. Cybersecurity education is important and can be brought into the curriculum through guidelines that will facilitate teaching and prepare students in cybersecurity competencies.

Methods of teaching

The objective of this question is to obtain an understanding of what lecturing methods are preferred for teaching a subject like cybersecurity. The teaching methods listed (e.g., lectures, discussions, role-playing, e-learning) represent distinct and independent methods of teaching rather than reflecting a single underlying construct. Cronbach's alpha assumes the items are related and measure the same concept, which may not be the case here. The highest standard deviation obtained was 1,054; thus it is acceptable.

Table 5 provides the methods of teaching that were presented to accounting academics.

TABLE 5 Methods of teaching.

Statement	Mean	Standard deviation
Lectures	3.93	0.877
Discussion	4.17	0.629
Working in small groups with other students	3.85	0.963
Guest speakers who are experts in cybersecurity	4.71	0.461
Case studies	4.34	0.728
Role-playing	3.80	1.054
E-learning (an online course)	4.00	0.975

Source: SPSS output of questionnaire, own layout.

Discussion of the findings

Table 5 provides an overview of the results with regards to methods of teaching. The highest number of academics (94%) agreed that expert guest speakers that come and speak to students is an effective way of integrating cybersecurity (mean = 4.71). Other areas such as case studies (mean = 4.34, 87%), discussion (mean = 4.17, 83%), and an online course (mean = 4.00, 80%), were all indicated as good teaching methods.

Lower scores (mean below 4) were obtained in lectures (mean = 3.93), working in small groups (mean = 3.85) and role-playing (mean = 3.80). This equates to 79%, 77%, and 76% of academics, respectively, that are in agreement with these teaching methods. These results indicate a strong preference for engaging and interactive teaching methods but suggest a need to re-evaluate traditional lectures and group work to improve their effectiveness. Academics might consider incorporating more innovative approaches to foster better student engagement and learning outcomes in these areas.

Additional comments by the academics

Academics commented mainly on the importance of making cybersecurity education practical as well as the importance of engaging with experts:

> *"Liaising with stakeholders or industry experts enhances understanding specific concepts and a practical application of work being covered in the course."*
>
> *"Effective cybersecurity education requires a versatile and inclusive approach that incorporates practical experiences, diverse perspectives from various fields, continuous learning opportunities, ethical considerations, and collaborative learning. By utilizing such teaching methods, educators can equip students with the knowledge and skills to become proficient cybersecurity professionals who are capable of dealing with the complex and ever-evolving cyber threats of the digital age."*
>
> *"Cybersecurity is important for professional and personal reasons and needs to be practically understood in order to be implemented. Less theoretical and more practical teaching is necessary."*

Source: Questionnaire data.

TABLE 6 Year of study.

Statement	Year	Number	%	Percentage of cases
Where should cybersecurity technical competencies be taught?	1st year	26	24.1%	63.4%
	2nd year	27	25.0%	65.9%
	3rd year	31	28.7%	75.6%
	Postgraduate	24	22.2%	58.5%
Total		108	100%	263.4%

Source: SPSS output of questionnaire, own layout.

Academics believe that, due to their lack of knowledge of cybersecurity subject matter, lectures were not preferred compared to bringing in an expert, which is in line with the literature (Zhang et al., 2020). Case studies develop students' ability to think critically about the subject matter, especially in an area like cybersecurity; moreover, students' reflective ability is developed as indicated in the literature (Ballantine and Larres, 2004). On the other hand, discussions develop behavior and develop familiarity with concepts in cybersecurity (Ismail and Rasheed, 2019).

Whilst online courses ranked highly, with an already full curriculum, it becomes difficult to develop a specially designed course. However, this method makes sense in an online-based curriculum (Strauss-Keevy, 2014). Working in small groups and role-playing are areas that can be added to projects, but not within class settings, mainly due to time constraints in terms of content that needs to be covered; hence, these items ranked lower (Rebele and St. Pierre, 2019).

Discussion of the findings

In the table, "cases" refers to the number of unique participants who responded to the question. Since participants could select multiple options, the percentage of cases shows the proportion of respondents (cases) who chose each option, relative to the total number of participants (being 41).

Most academics indicated that cybersecurity should be included in every year of study (1st, 2nd, 3rd and post-graduate). Table 6 indicates that participants had varying preferences regarding when cybersecurity technical competencies should be taught within the curriculum, with 24.1% of the total responses (63.4% of cases) suggesting the first year, 25.0% (65.9% of cases) favoring the second year, and 28.7% (75.6% of cases) showing the strongest preference for the third year, which likely reflects a belief that students would be more academically prepared at this stage. Additionally, 22.2% of responses (58.5% of cases) supported introducing these competencies at the post-graduate level, highlighting the belief that more advanced technical skills are suited for specialized education. Overall, the percentages indicate that many participants selected multiple stages, emphasizing the need for cybersecurity education to be integrated throughout the curriculum.

Comments from academics supported this and are discussed below.

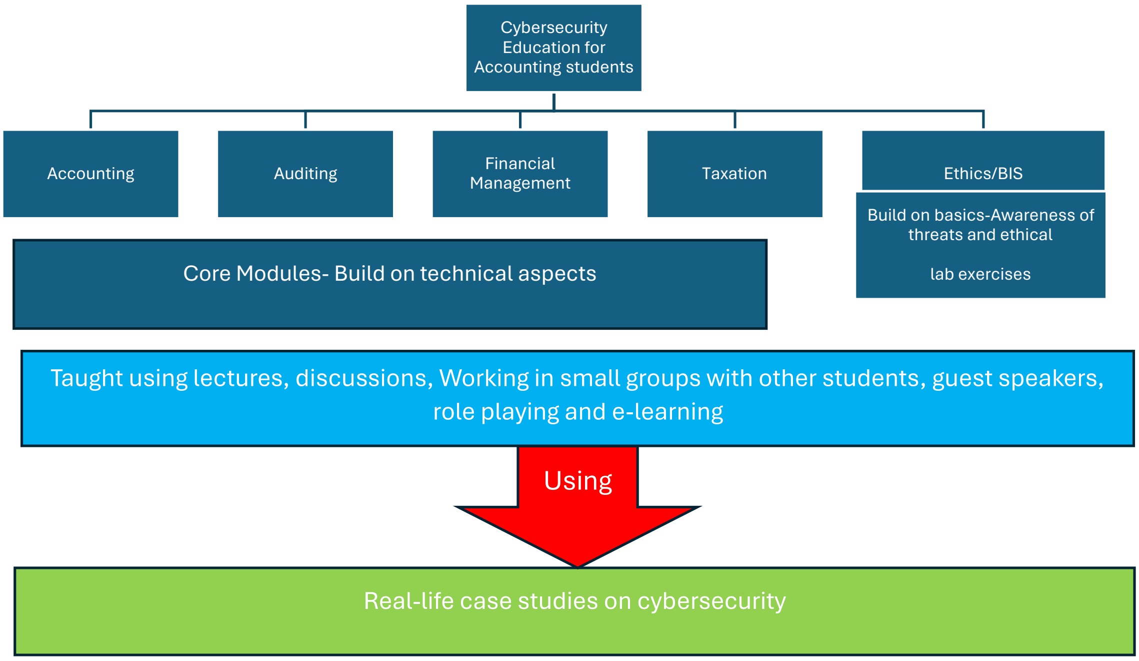
Cybersecurity Education for Accounting students
Accounting
Auditing
Financial Management
Taxation
Ethics/BIS
Build on basics-Awareness of threats and ethical
lab exercises
Core Modules- Build on technical aspects
Taught using lectures, discussions, Working in small groups with other students, guest speakers, role playing and e-learning
Using
Real-life case studies on cybersecurity

FIGURE 1
Integration of cybersecurity education in an accounting curriculum. Source: Own compilation.

Additional comments by the academics

> *"Cybersecurity should definitely be included in the accounting curriculum, and I think it will be beneficial to include throughout the accounting curriculum, thus from 1st to 3rd year and Honors. It should either be in the form of a business system module which the students will have from 1st to 3rd year, or if this is not possible, included in the various core modules. However, I think given the importance of cybersecurity as a result of the 4IR, this will have to become one of the core modules in the accounting curriculum."*
>
> *"Best taught in a course like Business Information Systems (BIS) and then engrained in all other modules, building on what was taught in BIS."*
>
> *"Cybersecurity should gradually be incorporated into the Accounting syllabus."*
>
> Cybersecurity should definitely be included in the accounting curriculum and I think it will be beneficial to include throughout the accounting curriculum thus from 1st - 3rd year and Honors. It should either be in the form of a business system module which the students will have from 1st to 3rd year or if this is not possible included in the various core modules.
>
> *It should be included throughout the accounting curriculum*

Source: Questionnaire data.

These findings agree with the literature in that cybersecurity should be spread throughout the curriculum and it should be staggered, thus lessening the burden of an already full curriculum, while ensuring that students receive a comprehensive understanding of the subject (Meyer, 2021).

Recommendations

- ➢ To manage curriculum overload, various cybersecurity competencies can be embedded throughout the curriculum.
- ➢ Introducing cybersecurity topics must avoid overloading students; content should be integrated within existing modules (e.g., embedding "data security" into auditing, or "cyber threats" into accounting information systems).
- ➢ Faculty development programs and Partnerships with IT/cybersecurity departments can provide guest lectures or co-teaching opportunities (e.g., courses, workshops, industry certification).
- ➢ Students should have access to lab facilities where practical cybersecurity aspects can be embedded e.g., in a module like BIS that already makes use of a lab facility.

The gradual integration of cybersecurity concepts allows students to engage with the content early in their academic careers and will embed the concepts, deepening their understanding. This is illustrated in Figure 1. Appendix 2 provides a mapping of competencies to various accounting modules to assist with integration into the accounting curriculum.

Conclusion

This study provides valuable insights into accounting academics' perspectives and understanding of cybersecurity in the accounting curriculum. The findings of this study indicate that accounting academics do not understand cybersecurity fully and require guidance when it comes to incorporating the topic. The study identified 19 cybersecurity competencies that can be incorporated into the accounting curriculum.

Various teaching methods such as lectures, discussions, working in small groups with other students, guest speakers that are experts in cybersecurity, case studies, role-playing and e-learning (an online course) are considered as methods that can be used to teach cybersecurity. Real-life case studies will add additional value in providing students with the required understanding. Further steps can include developing the accounting curriculum to align competencies with existing modules, and designing an assessment plan to evaluate students' knowledge and application of cybersecurity competencies.

The study provides a guideline in terms of how cybersecurity can be incorporated into the curriculum, through the various competencies, and can be ingrained through all years of studies (1st-post graduate studies), in ensuring that students receive a solid foundation with regard to cybersecurity education.

Limitations are noted. This study focused on accounting academics at a single university, which may limit the generalizability due to variations in curriculum structure, faculty expertise, and academic demographics across universities, and by self-reported data that may not fully capture a holistic view. Future studies should involve multi-site replication (inclusion of other universities offering accounting programs) and longitudinal evaluation of student learning outcomes, including assessments of faculty development impact and progression of cybersecurity competencies throughout the accounting program. In addition, future research could explore how emerging technologies such as AI and blockchain are being addressed within accounting education, alongside cybersecurity, to ensure students are well-prepared for a digital economy.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

Ethical clearance was received from the University of Johannesburg, with Ethical Clearance Number SAREC20240222/01.

Author contributions

PR: Writing – original draft. BM: Writing – review & editing. RS: Writing – review & editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/feduc.2025.1689273/full#supplementary-material

References

ACCA Global (2022). *Cybersecurity and the Accounting Sector | ACCA Global*. Available online at: https://www.accaglobal.com/uk/en/technical-activities/uk-tech/in-practice/2021/August/cybersecurity-and-the-accounting-sector.html (Accessed July 6, 2022).

AICPA (2021). *Accounting Program Curriculum Gap Analysis*. New York, NY: AICPA.

Alam, G. M. (2021). Does online technology provide sustainable HE or aggravate diploma disease? Evidence from Bangladesh—a comparison of conditions before and during COVID-19. *Technol. Soc.* 66:101677. doi: 10.1016/j.techsoc.2021.101677

Albuquerque, F., and Dos Santos, P. G. (2023). Recent trends in accounting and information system research: a literature review using textual analysis tools. *FinTech*. 2, 248–274. doi: 10.3390/fintech2020015

Aldawood, H., and Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*. 11:73. doi: 10.3390/fi11030073

Ali, W. (2020). Online and remote learning in higher education institutes: A necessity in light of COVID-19 pandemic. *High. Educ. Stud.* 10, 16–25.

Baker, M. (2016). *Striving for Effective Cyber Workforce Development*. Software Engineering Institute. Available online at: https://resources.sei.cmu.edu/library/asset-view.cfm (Accessed August 5, 2025).

Ballantine, J. A., and Larres, P. M. (2004). A critical analysis of students' perceptions of the usefulness of the case study method in an advanced management accounting module: the impact of relevant work experience. *Account. Educ.* 13, 171–189. doi: 10.1080/09639280410001676885

Barac, K., and Du Plessis, L. (2014). Teaching pervasive skills to South African accounting students. *S. Afr. Bus. Rev.* 18, 53–79. doi: 10.25159/1998-8125/5645

Bartley, E. D. (2023). "Professional competencies for student success in an increasingly global, digital, and virtual world," in *The Past, Present, and Future of Accountancy Education and Professions* (Hershey, PA: IGI Global), 153–175.

Berniak-Wozny, J., Plebańska, M., and Wójcik-Jurkiewicz, M. (2023). University students' perception of employability and workability skills for the workplace in the digital era. *Sci. J. Bielsko-Biala School Fin. Law* 27, 39–45. doi: 10.19192/wsfip.sj4.2023.5

Bérubé, J., and Gendron, Y. (2022). Through students' eyes: case study of a critical pedagogy initiative in accounting education. *Account. Educ.* 31, 394–430. doi: 10.1080/09639284.2021.1997768

Boss, S. R., Gray, J., and Janvrin, D. J. (2022). Accountants, cybersecurity isn't just for "techies": incorporating cybersecurity into the accounting curriculum. *Issues Account. Educ.* 37, 73–89. doi: 10.2308/ISSUES-2021-001

Bressler, L., and Pence, D. (2019). Skills needed by new accounting graduates in a rapidly changing technological environment. *J. Organ. Psychol.* 19, 22–31. doi: 10.33423/jop.v19i2.2043

Burrell, D. N. (2022). "Teaching graduate technology management students with innovative learning approaches around cybersecurity," in *Research Anthology on Advancements in Cybersecurity Education* (Hershey, PA: IGI Global), 491–500.

Business Day (2020). "UJ leads the 4IR teaching revolution in accounting," in *Business Day*. Available online at: https://www.businesslive.co.za/bd/business-and-economy/2020-09-29-native-uj-leads-the-4ir-teaching-revolution-in-accounting/#:$\sim$:text=Prof%20Amanda%20Dempsey%20is%20senior,embraced%20this%20wave%20of%20development (Accessed May 24, 2023).

Cameron, E. A., and Marcum, T. M. (2019). Why business schools must incorporate cybersecurity into the business curriculum: preparing the next generation for success. *J. High. Educ. Theor. Pract.* 19, 25–33. doi: 10.33423/jhetp.v19i4.2199

Chizanga, M. K., Agola, J., and Rodrigues, A. (2022). Factors affecting cyber security awareness in combating cyber crime in Kenyan Public Universities. *Int. Res. J. Innov. Eng. Technol.* 06, 54–57. doi: 10.47001/IRJIET/2022.601011

Chowdhury, N., and Gkioulos, V. (2023). A personalized learning theory-based cyber-security training exercise. *Int. J. Inform. Secur.* 22, 1531–1546. doi: 10.1007/s10207-023-00704-z

Churyk, N. T., Eaton, T. V., and Matuszewski, L. J. (2024). Accounting education literature review. *J. Account. Educ.* 67:100901. doi: 10.1016/j.jaccedu.2024.100901

CIMA (2018). *2019 CIMA Professional Qualification Syllabus*. United Kingdom: CIMA.

Cook, J. V., Dickinson, H. O., and Eccles, M. P. (2009). Response rates in postal surveys of healthcare professionals between 1996 and 2005: An observational study. *BMC Health Serv. Res.* 9:160. doi: 10.1186/1472-6963-9-160

Corriss, L. (2010). "Information security governance: Integrating security into the organizational culture," in *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (New York, NY: ACM), 35–41.

Crean, A., and Carroll, N. (2022). "Developing information systems for the contemporary accounting profession: Challenges and recommendations," in *The Routledge Handbook of Accounting Information Systems* (Milton Park: Routledge), 50–62.

Dore, A. C., and Murphy, M. (2022). *The Impact of the Accounting Curriculum on Alumni Professional Success*. Available: https://www.proquest.com/dissertations-theses/impact-accounting-curriculum-on-alumni/docview/2667737721/se-2?accountid=13425

Douglas, S., and Gammie, E. (2019). An investigation into the development of non-technical skills by undergraduate accounting programs. *Account. Educ.* 28, 304–332. doi: 10.1080/09639284.2019.1605532

Ebaid, I. E. S. (2022). An exploration of accounting students' attitudes toward integrating forensic accounting in accounting education. *Int. J. Law Manag.* 64, 337–357. doi: 10.1108/IJLMA-06-2021-0154/FULL/PDF.

Fakoya-Michael, S. A., and Fakoya, M. B. (2020). Library usage by university accounting students: a comparison of contact and open distance learning institution in South Africa. *J. Acad. Librariansh.* 46:102093. doi: 10.1016/j.acalib.2019.102093

Ghani, E. K., and Muhammad, K. (2019). Industry 4.0: employers' expectations of accounting graduates and its implications on teaching and learning practices. *Int. J. Educ. Pract.* 7, 19–29. doi: 10.18488/journal.61.2019.71.19.29

Grech, B. P. (2022). *Understanding Student Perspective of Undergraduate Cybersecurity Programs and Experiences Across Christian Colleges and Universities.*

Greene, D., and David, J. L. (1984). A research design for generalizing from multiple case studies. *Eval. Prog. Plann.* 7, 73–85. doi: 10.1016/0149-7189(84)90027-2

Gulin, D., Hladika, M., and Valenta, I. (2019). Digitalization and the Challenges for the Accounting Profession. *ENTRENOVA-ENTerprise REsearch InNOVAtion*. 5, 428–437.

Gurin, P., Dey, E., Hurtado, S., and Gurin, G. (2002). Diversity and higher education: theory and impact on educational outcomes. *Harvard Educ. Rev.* 72, 330–367. doi: 10.17763/haer.72.3.01151786u134n051

Hadgraft, R. G., and Kolmos, A. (2020). Emerging learning environments in engineering education. *Aust. J. Eng. Educ.* 25, 3–16. doi: 10.1080/22054952.2020.1713522

Heale, R., and Twycross, A. (2018). What is a case study?' *Evid. Based Nurs.* 21, 7–8. doi: 10.1136/eb-2017-102845

IESBA (2022). Technology Landscape: Focus on Data Governance. New York, NY: IESBA.

IFAC (2023). *IFAC Technology Matrix*. New York, NY: IFAC.

Ismail, S., and Rasheed, Z. (2019). Influence of ethical ideology and emotional intelligence on the ethical judgement of future accountants in Malaysia. *Meditari Account. Res.* 27, 805–822. doi: 10.1108/MEDAR-04-2018-0326

Jackson, D., and Meek, S. (2021). Embedding work-integrated learning into accounting education: the state of play and pathways to future implementation. *Account. Educ.* 30, 63–85. doi: 10.1080/09639284.2020.1794917

Jackson, D., Michelson, G., and Munir, R. (2023). Developing accountants for the future: new technology, skills, and the role of stakeholders. *Account. Educ.* 32, 150–177. doi: 10.1080/09639284.2022.2057195

Jeffryes, J., and Lafferty, M. (2012). Gauging workplace readiness: assessing the information needs of engineering co-op students. *Issues Sci. Technol. Librariansh.* 69, 1–7. doi: 10.29173/istl1548

Jerman BlaŽič, B., and Jerman BlaŽič, A. (2022). Cybersecurity skills among European high-school students: a new approach in the design of sustainable educational development in cybersecurity. *Sustainability* 14:4763. doi: 10.3390/su14084763

Johansson, R. (2007). On case study methodology. *Open House Int.* 32, 48–54. doi: 10.1108/OHI-03-2007-B0006

Kee, H. Y. (2024). "Incorporating digital skills in accounting education," in *Digital Transformation in Accounting and Auditing: Navigating Technological Advances for the Future* (Berlin: Springer), 3–27.

Keevy, M. (2022). *Capacity Development of Accounting Educators: A Case Study of Developing Countries*. (Doctoral dissertation). Johannesburg, Gauteng: University of Johannesburg.

Kelly, A. V. (2009). *The Curriculum: Theory and Practice*. Thousand Oaks, CA: Sage Publications.

Khan, M. A., and Law, L. S. (2015). An integrative approach to curriculum development in higher education in the USA: a theoretical framework. *Int. Educ. Stud.* 8, 66–76.

Kisaalita, W. S., Muyanja, C. K., and Mativo, J. M. (2022). Undergraduate students' short-term inquiry-or design-based overseas experiences enhance their global engagement acumen. *Eur. J. Eng. Educ.* 47, 1216–1228. doi: 10.1080/03043797.2022.2134761

KPMG (2022). *KPMG US CEO Reveals How to Get Hired There*. Available online at: https://www-businessinsider-com.cdn.ampproject.org/c/s/www.businessinsider.com/kpmg-us-ceo-how-to-get-hired-ideal-job-candidates-2022-5?amp (Accessed May 27, 2022).

Kumar, S., Benigni, M., and Carley, K. M. (2016). "The impact of US cyber policies on cyber-attacks trend," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. Piscataway, NJ: IEEE, 181–186.

Leidig, P. M., and Salmela, H. (2022). The ACM/AIS IS2020 Competency Model for Undergraduate Programs in Information Systems: a Joint ACM/AIS Task Force Report. *Commun. Assoc. Inf. Syst.* 50:25. doi: 10.17705/1CAIS.05021

Loots, E., Oberholster, J., Steyn, A., Antonites, A., van der Merwe, A., Merino, A., et al. (2024). *Rethinking Commerce Education in South Africa: The Case for Change to Develop Future-Fit Business Leaders*. Cape Town: AOSIS. doi: 10.4102/aosis.2024.BK454

Malan, M., and van Dyk, V. (2021). Perceived pervasive skills acquired through educational games in an accounting undergraduate degree. *J. Econ. Fin. Sci.* 14, 1–11. doi: 10.4102/jef.v14i1.555

Matthysen, M., and Harris, C. (2018). The relationship between readiness to change and work engagement: a case study in an accounting firm undergoing change. *SA J. Human Resour. Manage.* 16, 1–11. doi: 10.4102/sajhrm.v16i0.855

Mendlowitz, E. (2022). Growing today's accounting businesses. *CPA J.* 92, 70–71. doi: 10.2308/cpaj-2022-70

Meyer, C. (2021). Fit cybersecurity into your accounting courses—Extra Credit. *J. Account*. Available online at: https://www.journalofaccountancy.com/newsletters/

extra-credit/fit-cybersecurity-into-accounting-courses.html (Accessed February 8, 2023).

Mgaiwa, S. J. (2021). *Fostering Graduate Employability: Rethinking Tanzania's University Practices* (Los Angeles, CA: SAGE Publications), 11.

Mijwil, M., Salem, I. E., and Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: a comprehensive review. *Iraqi J. Comput. Sci. Mathematics* 4, 87–101. doi: 10.52866/ijcsm.2023.01.01.008

Montgomery, J. J. G. (2022). Assessing the digital technology competencies of certified public accountants: a gaze into ilokano workplace context. *Univ. J. Educ. Res.* 1, 26–36. doi: 10.5281/zenodo.6937848

Mphahlele, L. (2023). A framework for developing critical thinking skills for accounting students. (Doctoral Dissertation). University of Johannesburg, Johannesburg.

Mujiono, M. N. (2021). The shifting role of accountants in the era of digital disruption. *Int. J. Multidiscip. Appl. Bus. Educ. Res.* 2, 1259–1274. doi: 10.11594/10.11594/ijmaber.02.11.18

Nulty, D. D. (2008). The adequacy of response rates to online and paper surveys: what can be done? *Assess. Eval. High. Educ.* 33, 301–314. doi: 10.1080/02602930701293231

Panja, S. (2018). Creative methods of teaching accountancy-Its impact. *SocArXiv*. doi: 10.31235/osf.io/n3y26

Pasewark, W. R. (2021). Preparing accountants of the future: Five ways business schools struggle to meet the needs of the profession. *Issues Account. Educ.* 36, 119–151. doi: 10.2308/ISSUES-19-025

Paulsson, V., and Brady, M. (2022). "Accounting information systems: supporting business strategy," in *The Routledge Handbook of Accounting Information Systems* (Abingdon: Routledge), 285–300.

Rajgopal, S. (2021). Integrating practice into accounting research. *Manage. Sci.* 67, 5430–5454. doi: 10.1287/mnsc.2020.3590

Rebele, J. E., and St. Pierre, E. K. (2019). A commentary on learning objectives for accounting education programs: the importance of soft skills and technical knowledge. *J. Account. Educ.* 48, 71–79. doi: 10.1016/j.jaccedu.2019.07.002

Rensburg, I. (2020). *Serving Higher Purposes: University Mergers in Post-Apartheid South Africa*. Stellenbosch: African Sun Media.

Rîndaşu, S-. M. (2017). Emerging information technologies in accounting and related security risks – what is the impact on the Romanian accounting profession. *J. Account. Manage. Inform. Syst.* 16, 581–609. doi: 10.24818/jamis.2017.04008

Roohani, S., and Zheng, X. (2019). "Using ten teaching modules and recently publicized data-breach cases to integrate cybersecurity into upper-level accounting courses," in *Advances in Accounting Education: Teaching and Curriculum Innovations* (Bingley, UK: Emerald Publishing Limited) 113–125.

Saadeh, A. (2019). A stakeholder approach to the development of a framework for forensic accounting education within the Jordanian context. Available online at: https://researchcommons.waikato.ac.nz/handle/10289/12945 (Accessed November 4, 2022).

SAICA (2022). *CA2025—CA of the Future*. Available online at: https://ca2025.co.za/ (Accessed July 12, 2022).

SAIGA (2023). *Registered Government Auditor Competency Framework 2023*. Available online at: https://www.saiga.co.za/saiga/wp-content/uploads/2023/06/SAIGA-Competency-Framework-2023.pdf (Accessed October 28, 2024).

Sheats, R. D., and Shane Pankratz, V. (2002). Understanding distributions and data types. *Sem. Orthodont.* 8, 62–66. doi: 10.1053/sodo.2002.32075

Srinivasan, S. (2013). Digital forensics curriculum in security education. *J. Inform. Technol. Educ. Innov. Pract.* 12, 147–157. doi: 10.28945/1857

Stake, R. E. (2013). *Multiple Case Study Analysis*. New York, NY: Guilford press.

Strauss-Keevy, M. (2014). *Perceptions of accounting academics on the delivery of pervasive skills under the SAICA Competency Framework*. University of Johannesburg (South Africa).

Sutherland, E. (2020). The fourth industrial revolution—the case of South Africa. *Politikon*. 47, 233–252. doi: 10.1080/02589346.2019.1696003

Syomwene, A. (2020). Curriculum theory: characteristics and functions. *Eur. J. Educ. Stud.* 7, 17–28. doi: 10.46827/ejes.v7i12.3514

Tauchman, E. R. (2021). *From Finance and Risk to Cybersecurity | CompTIA*. https://www.comptia.org/blog/from-financial-and-risk-analysis-to-cybersecurity (Accessed June 21, 2022).

Terblanche, E. A. J., Shuttleworth, C. C., van Rooyen, A. A., and Masela, R. N. (2023). Critical thinking: Stakeholder expectations and challenges for Accountancy educators. *S. Afr. J. Account. Res.* 37, 225–244. doi: 10.1080/10291954.2022.2148925

Tharapos, M. (2022). Opportunity in an uncertain future: reconceptualising accounting education for the post-COVID-19 world. *Account. Educ.* 31, 640–651. doi: 10.1080/09639284.2021.2007409

van Oorschot, P. C. (2020). *Computer Security and the Internet*. Berlin: Springer.

Wolk, C., and Nikolai, L. A. (1997). Personality types of accounting students and faculty: comparisons and implications. *J. Account. Educ.* 15, 1–17. doi: 10.1016/S0748-5751(96)00041-3

Woods, M., Paulus, T., Atkins, D. P., and Macklin, R. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS. ti and NVivo, 1994–2013. *Soc. Sci. Comput. Rev.* 34, 597–617. doi: 10.1177/0894439315596311

Zhang, Y., Xiong, F., Xie, Y., Fan, X., and Gu, H. (2020). The impact of artificial intelligence and blockchain on the accounting profession. *IEEE Access*. 8, 110461–110477.

Zhang-Kennedy, L., and Chiasson, S. (2022). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Comput. Surv.* 54, 1–39. doi: 10.1145/3427920